Sensors Workshop Notes

Day 1

8:30-8:45: Intro, Bryan Gorman, ORNL

Announced that conference sponsors were himself, Kang Lee, and Dave Godso. Godso absent but represented by Josh Pressnell.

8:45-9:00: Welcome, John Doesburg, ORNL

Gave briefing on Oak Ridge National Laboratory. Emphasized need for fast sensing of CBRN threats.

9:00-9:15: Net-Ready Sensors for the DoD: MG Steve Reeves, JPEO-CBD

Presented in absentia via video; Strongly supported conference goal of bringing together different groups to harmonize Department of Defense (DoD) requirements.

He is from Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD). Group does DoD research & development and acquisition of chem-bio technology.

Wanted sensors to be like Bluetooth and USB: to allow unrelated devices to talk with each other, to make plugging in new applications thoughtless, to use easily recognizable and standard interfaces, to be standardized by standards body of private companies, to be backwards compatible

Need to learn lessons from September 11 and Katrina: national preparedness is crucial; military capabilities and communications must be integrated.

Touted Unified Command Suite, used by the National Guard during Katrina, as one of the few success stories: Its network was the key; it synchronized with major programs and integrated interdependent systems in a network. Should be true of all networks.

Standards always evolving, never a stable environment or well-defined requirements.

Need a continual access to data, shared awareness, and self-synchronization,

Executing these standards has three requirements: 1. sufficient processing power to be real-time 2. simple, concise, and useful enough to make it worthwhile for first-responders 3. cheap enough to be worth it

Network needs to be available throughout chain of command;

Need common architecture for sensors networks; He calls it modularity: components then modular then systems

Need common data sets, They exist and are commercially available.

In event of attack DoD and civil forces need to be communicating with each other and with national leadership, biological attack not discovered until symptoms, need to rapidly identify exposed and infected, time is critical factor, need systems already in place, need environmental sensors and surveillance, use modeling and simulation to identify area of contamination, need to bring in weather and medical data, automated tools give most info to decision makers.

Modules should be standards-based, and usable on multiple platforms and applications; capable of being used by untrained people.

Service Oriented Architecture (SOA) based on standards keeps networks from being locked in by proprietary software.

Summary: Right info to decision makers at right time, common software, no unique protocols, PnP, and reduced cost of maintenance.

9:15-10:00: CBRN Data Model, Tom Johnson, JPM IS Data APM

He created the CBRN data model, a service oriented architecture.

Joint Requirements Office and Joint Program Executive Office (JPEO) signed agreement, wanted to focus on common data layer, mandated use of data model, enables interoperability and reuse, physical representation of logical model, also can be a conceptual model of battle space.

Wanted to deal with PnP model in changing environment, scalable and adaptive, XML schema that is 1:1 correspondence with data model, fulfills net centricity of DoD goals, lingua franca of community, define syntax that systems should use to describe aspects of systems.

Resembles physical database, no real physical base but can create it.

History of model, 2002 white paper written on common data representation, 2003 development begun, preliminary drafts, 2004 1.0 and 1.1 released, most major areas present in 1.0, JC3DIM, C2DIM was analyzed and felt that it was useful but that it was not secure enough for CBRN community, C2DIM is maybe 20 percent of data model

1.1 added: agent stimulant knowledgebase (ASK) attributes, ATP-45 attributes, metadata of entities and attributes, adopted UK spelling, ATP-45 Panel endorsed data model as ‘Extended C2IEDM’, used for data exchange within NATO community

1.2 and 1.3 added: enhanced Configuration Management tracking, significant remodeling of material properties, added CBRN equipment entities, radiation exposure guidelines, many HPAC variables: had to reverse engineer; now has all of them

JRO issued JSAP Tasker to review the data model; resulted in 266 change proposals

Significant work done for chemical sensors and biological collectors, Guardian and RPM sensors; Originally had Guardian bias, now more generic.

Can cut and dice population temporally and spatially.

Complexity: 446 entities, 3,611 attributes, 1317 relationships, can query to make simpler

1.4 remodeled CBRN Event Subtypes: nuclear facility incident is now a subtype of radiological event, change made based on community input; Radiation Portal Monitor entities have been added. Support for Remote sensor panels and cameras using RPMs; Geographic feature; Material properties; Concentration also based on FM 3-11.9

Sensor generalization continually being worked on.

Future additions: decontamination, medical document/binary objects, representative sample data

ERWIN Data Model is logical model, CBRN XML Schema, SGQ Scripts, Documentation

Object info, type time status and reporting data (timestamp),

Spatial info

Metadata

Action info

Tree of CBRN events, can work with actual incident at the level of an individual room,

Weather and terrain inputs are exogenous to data model.

Based on ASK database from ECDC; categories are FM 11 3-9.

Erwin representation of sensors, sensor is a type of object, broken down into electronic components, and type

Data dictionary is published along with data model, gives info about attributes and entities sued, valid values for different sensors.

Believes data model would have saved $5 million to $10 million for DoD development, Guardian suggested that they saved $1 million from model.

Self-contained model, most valuable is that it gathers in one place all the algorithms that are used in various systems, links to relevant equations and user defined attributes.

Service Oriented Architecture (SOA):

Enabler of service enabled infrastructure needed for service provider and consumers

Advantages: allows customers direct access to info

Wants to develop with standard syntax, simply using XML does not guarantee interoperability.

Key enabler to exchange seamless documents

Independent of any platform, does not require platform to be deployed with application.

Data exchange XML SMK: CBRN Data Model schema breaks down into XML tools then classes are automatically generated and translated into JAR files.

Summary: Essential to interoperability in systems, an incremental proactive approach for both legacy and new systems, supported by an implementation infrastructure, common tools and techniques, implementation guidance and requirements are available, made for a collaboration environment

What system needs: Transforming SSA builds a series of implementation tools, also want guidance for building translators, are building translators for old systems, to make old system data for XML coding, codes from specific groups: need XML translation, for other groups to use, want people to accept their syntax, give fodder to people who are using translator, SSA develops best practices for translating, they are doing translation.

QUESTIONS:

RICK MCMULLEN: Are they tracking the evolution of attributes taken from other models?

REPLY: We track them, 15- 25 percent of the CBRN DM is based on JC IEDM, which is corporate model for NATO. Worked with experts to borrow data schemes but have tried to not build anything new: wanted to use models that work and was tired of reinventing the wheel for data models.

Are having a series of meetings on how to institute configuration management, that is, how to deal with change over time in systems that it borrowed from. User defined properties change much of the model's information; document who changes attributes and when it is changed:

BRAND NIEMAN: Common XML schema gives common computer language, but how does it fit different spoken languages?

REPLY: British English is language of NATO and is what CBRN DM uses. NATO people he has worked with all used British English without problems.

10:15-11:00 ANSI N42.42, George Lasche, Sandia National Laboratories

N42.42 is the ANSI standard for data format for radiation detectors used for homeland security. It is required by DHS for all radiation detection equipment that DHS will purchase.

He was technical chair for development committee.

His job: Emergency nuclear response and analytical nuclear physics.

Emergency responders must be able to analyze data that is sent to them in over 50 different formats and format variations from an increasing number of manufacturers of hand held instruments to measure spectra from radiation sources. He developed CAMBIO, software to translate data files from any of theses different formats to standard formats that are useful for analysis, including the new DHS-sponsored N42.42 ANSI Standard data format.

The N42.42 format is a derivative of XML. The use of XML enables "validation" of data files through XML schema. This is important because it enables users to easily make sure that the data they write conforms to the syntax of the standard.

The N42.42 format has passed all the requirements to be finalized as an ANSI Standard and is now awaiting proofreading and publication by the IEEE.

The N42.42 had the following requirements:

1. Readability on notepad or WordPad – essential for emergency response;
2. Compatibility with accepted international standards for data representation to the broadest extent possible;
3. Must be able to validate content: XML ensures that users do not inadvertently deviate from the standard.
4. Extensibility: provide for unforeseen future needs and as yet unknown requirements, only put things needed for more than one manufacturer, one could add namespace of their own, did not want to aid anyone's commercial business

N42.42 accommodates all 5 of the basic homeland security instrument types: 5 classes, 42.32-35 and 38

N42.42 file sizes are generally smaller than their binary counterparts, contrary to popular pre-conceived notions about the use of XML, which is expressed in ASCII. As an example, the same file written in Canberra's CNF format which was originally 63 kB, and in Ortec's CHN format at 33 kB, when written in N42 is only 22kB.

The N42.42 file structure:

1. Line that says this is XML – optional, needed only for validation
2. schema to validate that this is XML – also optional, needed only for validation
3. the first element <N42InstrumentData> is the parent of everything within file, name; as an example, a "Cambio" namespace was provided to show extensibility
4. Measurements – more than one are allowed
5. Spectrum elements – more than one are allowed per Measurement
6. <StartTime> element – an example of a child element allowed only once

Summary: forward and backward compatibility, Human readable for emergencies, single format for all radiation detectors, not binary so easily passes servers scanning for viruses, file size economy, can be validated

Dr. Lasche performed a demonstration of coding in N42 format.

QUESTION: Is the N42.42 format used by all DHS vendors?

REPLY: The use of N42.42 is only beginning to be required. For legacy data, CAMBIO has a batch file conversion utility to translate from existing languages used by manufacturers. DHS requires the N42.42 format for radiation detection equipment they purchase. Recently a $1.2 billion contract was awarded for advanced spectrometric portals in which the vendors are required to use the N42.42 format.

QUESTION: If analyzing readings that were made long ago and recorded by other software will CAMBIO present information about the original data source and the software that initially interpreted it?

Yes. Drag any spectrum onto the CAMBIO icon and Cambio will automatically recognize any format, read and display the spectrum graphically. Cambio also has some tools for comparing spectra. Its batch processing capability allows the user to automatically convert many files at once to the N42 format.

Cambio is unrestricted and unclassified, distributed by FTP downloads with email notifications approximately every 6 weeks. Can email a request to receive it, no restrictions or fees.

A list of users is kept confidently so he can send out updates.

11:00-11:45: Common Alerting Protocol (CAP), Art Botterell, EM TC (OASIS)

With OASIS Emergency Management Technical committee.

Originally developed CAP because he needed a common data format to syndicate information around a number of systems for detecting tsunamis in Singapore.

CAP developed from consumer end first; how to deal with public: AIR; alerting, informing, reassuring, needs attention management and emotional element along with data format

State of Public warning: unrealized opportunities, many useful warning tools, people mistrust single-source warnings, confused by inconsistent messages so can't be inconsistent if use multiple sources, people are annoyed by irrelevant warnings: danger of them "tuning out", not desensitized by warnings but by irrelevant warnings

Opportunities: Much academic knowledge about how humans interpret warning messages; heightened awareness recently; most warning systems are now computer controlled: opportunity for integration

Missing Piece: need standard method to glue systems together; began working on a non-proprietary XML content standard for sharing alerts and warnings, backwards and forwards compatible, flexible geographic targeting of alerts, message update and cancellation features, phased times and expirations, and digital information management.

CAP Time-line:

November 2000, report

2001; mailing list worked on CAP, convened Partnership for Public Warning

2002-3, small scale test and field trial with little federal funding

2003; CAP data elements added to global Justice XML Data dictionary (now International Information Exchange Model)

2004: Cap 1.0 approved as OASIS standard

2005: DHS "Digital EAS" and other deployments, CAP 1.1 update adopted

Design Philosophy: Research based template for complete and effective messages: wanted to know how people would respond; used that as basis for design.

Consistent delivery to all audiences across all warning systems: need to hear the message three times before it gets their attention

Compatible with old systems

Simple for warning officials

Structure: an “envelope” identifies source of message for later references, message type, and other categories

Contains 0 or more info elements

Information: who what when where, why, so what

Wanted to unpack traditional ideas of priority, urgency, severity, certainty of quality of information, wanted to communicate uncertainty to public.

Uses multiple information blocks can be used for time-phased events, multi-lingual, multi-level (watch or warning) message.

Extensibility of XML would make essential elements lose meaning, so restricted CAP message to two forms, allowed for optional attachment of any additional (binary) data file.

Area: target specific areas for warnings, beyond political zones, can use plume model data to reduce spill of message, and assumes delivery system can deal with area.

Can run on location aware cell phones within area of warning: a company has commercialized this idea.

Need agreements on transport: web services vs. RSS feed, routing and buffering needed; if receive after issued but before it expires; Identity: Data Sources: Displays and Applications: Disclosure policies and Standards of Practice: above technical standards, need protocols for humans when issuing warnings, especially when information is deemed sensitive and uncertain.

Situational Awareness: Need more than just sensing events; need to find patterns within information, trends, and deviations, which allow anticipation of events.

Application of CAP to sensors: not focused on sensors, two years into development began to incorporate sensor data into design.

That said: was optimized for human interface, not best format for representing sensor data, good general purpose tool for next layer of wrapping for existing data sets

Relevance to conference: a bottom-up, open source development of standards without government funding, was not under official mandate until end, is example that that can be done, that ultimate goal is to reach public use, not just decision makers, COMMENT: for DoD wants to be able to give different versions of warnings for different levels of classification (e.g. public, police, Pentagon, White House)

1:00-1:45: EDXL-DE, Gary Ham, Battelle

Distribution is an XML schema composed of tags that allows characterization and identification of content, either standard or non-standard.

Approved by OASIS members in April 2006

Robust as you want set of tags for characterizing content for routing purposes, can be simple.

Single transport interface for multiple types of content.

Detailed characterization is powerful and expensive; DE application must accept all tags but does not have to use them.

Categorizes the message in many ways: message function, confidentiality, language, sender, recipient, keyword, target area.

Value list URN concept, in value list is name of a published list of values and definitions, and the content of value is a string denoting the value itself.

Content: abstract actual content from the interface; provides a stable, highly reusable interface, even if the data it processes change dramatically.

The standard provides a known, well-organized structure for location of content in the message.

Xpath process that you are looking for, and process each one individually at processor's end.

Levels of use:
Crawling: Connect mechanism for sharing

Walking: content, characteristics

Running: Rule-based, publish-subscribe, DE Routing

Crawl example: DHS Disaster management Program provides a production ‘crawl” interface as part of its Open Platform for Emergency Networks (OPEN). It works robustly in a high volume environment, only limited use of the many available DE tags.

Walking: involves two legs, both of which can be gradually strengthened, systems can implement appropriate processing to one standard at a time.

Can improve the granularity of the categorization of sent message, sender/receiver roles and geographic areas are important first considerations.

Content and characterization are legs
Content:
Client applications: client systems can use Xpath to find and process known content
Redistribution: network nodes can extract “known” content for separate forwarding.
Knowing content is first leg.

Characterization:
Importance determination, sub application distribution, initial rerouting rules,

If you build a message that makes sense, you can employ another system to do redistribution using full power.

RUN: client applications apply to services, provide interface for allowing post of published data

Redistribution: provides rule based routing capability based on DE structure.

Subscription required, as is post interface and user management for senders and receivers.

Walk or crawl systems can piggyback onto an EDXL router to get enhanced capability, PRICE: need to comply with router’s administrative registration VALUE: reuse of power for distribution without having to put all of the complexity on the edges (Let the router do it.)

Resiliency: you can still do it yourself.

NIMS: not a system, a concept of operations, consistent and well defined, how generally incident management will be done, must support a combo of networks used by USC: not any specific one.

EDXL-DE is an XML schema for communicating emergency information. It does not need to be wrapped in a SOAP envelope, but it can be.
Examples: from XML editor, will show a CAP 1.1 message within a DE that is stripped and posted to two different products.

Also wrapped N42 message to be sent in DE.

Can handle ciphers and signatures, has redundancy if misses one sender, it can still get DE to others.

1:45-2:30: WFS-T, Ron Lake, Galdos

Developed the concept for OGC's Geography Markup Language; President and CEO of Galdos systems

Web Feature Services: transactional.

Review of GML and WFS, for Sensor Data, and WFS/WRS/SensorNet.

Geography Markup Language: international standard of Open Geospatial Consortium and ISO.

GML is an XML grammar for describing geographic objects—a Data descriptive language for geographic content; a language to write "geographic" languages.

Written in XML Schema; is extensible.

Designed to support geographic transactions not just file transfer, not replacement for just sending file software, way for databases to interact with other databases to change their geographic information.

Borrowed from RDF, simple model Objects-properties-values; nested

Rich collection of base/primitive objects; inherently self-describing

Used by US DOT, Census Bureau, Euro Space Agency, Google KML, NATO, Shell Oil

It is a way of expressing schemas, can share with other people, can describe geographic elements within it

Provides lingua franca for data transport, and Spatial transaction (where sensors relate)

Can write down geospatial types, can use types (like road) to describe to a web service

Modeling Geography: Three general things: 1. discrete meaningful objects (Features) no concrete objects, you make objects (roads, dams, trucks, etc. known as Features. 2. distributions of quantities (COVERAGES) like temperature, roughness along road. 3. observations: act of measuring or observing, time when it took place, location, and result from observing,

GML in SensorNet context: airplane carrying camera, acquires picture, picture is coverage, in context of when taken and from where is observation; features derived from picture include school that is included in photo;

GML provides building blocks, reference systems, can create won coordinate system, can represent time instance and temporal dimensions, own clocks and calendars geometry: can express points, different surfaces

GML is being used in Germany to build 3d models of cities; topology; units of measure: meters, viscosity: set own definition for things like this;
Coverages would be remotely sensed images.

These are encoded in XML, can just use it to describe geometry and content of image so don't have to store in XML, can do it within seam.

SensorNet profile of GML: used to build application vocabulary, over 1,000 tags, if don't need can use a profiling tool that subsets only the core schemas that you need.

Then build a SensorNet vocabulary for application.

Then user or community of defined vocabulary.

GML Model

Each entity maps to an element, attributes are always children of entities, values are under attributes

Large number of primitives: over 600 pages spec, much of it dictionary.

Web feature service: vendor neutral interfaces to access geospatial information (GIS database) WFS client issues a request (in GML) for something (whatever it is they want is defined by GML) then get back a response in GML, it sends back information for whatever geographic thing they requested within an area, User never knows what underlying database is.

Queries that can be made are defined by web feature service specification; database does not have to have spatial data, can still make requests

Key: vendor neutral transaction across the internet; not just request, but a change of other database; send request (GML) insert road or bridge or modify feature, receive status information response defined by WFS interfaces, if roads taken out by attack: change of state could be changed and results received

Sensor is a type of observer can make requests and change them, perhaps status is sent back; if future sensors are GML aware they could skip gateway.

Been developing since 2000, current version 3.1.1; version 3.2 is complete; ISO 19136 is other issue

WFS is in v1.1; will be likely known as ISO 19143

Features of WFS 1.2; support GML 3.2; temporal operators— now supports Temporal DATA type(already in GML); better collection semantics; fine grained CML Object Support, Sort by product option.

Sensors are isolated; context determines real value of sensor data(context is metadata)

Web registry service: brings GML observations from WFS to one place, separate from web feature service.

2:30-3:15: XMPP, Boyd Fletcher, JFCOM

Extensible Messaging and Presence Protocol (XMPP) and Cross Domain Collaborative Information Environment (CDCIE)

Sensor data needs to be sent up to higher networks to get complete picture; transport mechanism could be XMPP

Goal is to develop a standards, based, non-proprietary, open source, secure, scalable collaborative information environment (CIE) to enable cost effective multinational information sharing in both single and cross domain environments, (CDCIE)

Testing initial version of CDCIE Chat is 2.1 which will be completing NSA CT&E in Oct 2006"; cross domain multi-user text chat, language translation, cross domain XML Guard

Future will have web services gateway, file transfer gateway, secure save, data sync guard; streaming data,.

Current Systems are the collaborative gateway and transverse client (formerly called Buddyspace)

Collaboration sensor perspective: if talking to sensors via XMPP, could use the CG to get to sensor data to the high side safely and the transverse client could be extended to provide a collaboration and visualization frontend to the sensor data.

OVERVIEW OF XMPP

Set of streaming XML protocols to exchange messages, started as protocol for interconnecting a wide variety of Instant Messenger (IM) systems

OPEN—protocols are free, open, public, well defined, XML based;
DECENTRALIZED: the architecture is similar to email

XMPP addresses resemble email addresses

SECURE: encrypted and unencrypted modes

One of three IM/Text Chat protocols approved by the IETF(Internet Engineering Task Force)

ON OCT 4 2004, XMPP suite was published: extensible messaging and presence protocol; RFC 3920-3

Client finds your server using DNS lookup; opens connection with that server then sends the message to the other client's server

XMPP consists of client to server and server to server protocols.

Usable on many operating systems: including Windows CE and Palm OS: useful for warfighter; works well on cell phones.

Firewall friendly; more secure collaboration tool than email; not generally susceptible to viruses; requires user security: Simple Authentication and Security Layer (SASL); Server based architecture allows all communications to be recorded and audited on server;

Other features: publish/subscribe, audio signaling, language translation, file transfer, web services, service discovery, stream compression, common alerting protocol.

Whiteboarding coming soon, many others defined as Jabber Enhancement Proposals at www.jabber.org/jeps

MITRE collaborative Data Objects: want data to be sent over a known format when targeting, do not want it to be misinterpreted; project to embed data in XMPP, collaborative data objects, free form but structured data in XML over XMPP, JEP will be submitted to Jabber Software Foundation.

Summary: Standard framework for talking with servers; Cross domain chat for different security classifications

3:30-4:15: Semantic Interoperability Community of Practice (SICoP), Brand Niemann, EPA

Used a collaborative wiki to implement Data Reference Model (DRM) 2.0

Metamodel is information about the model just as metadata is information about the data.

Just structured data in early versions: current version includes semi-structured and unstructured data

More metadata added equals better searching.

A reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details. (It does seek to provide a common semantics that can be used unambiguously across and between different domains)

Ontology approach provides both a conceptual data model and data architecture.

UDER Universal Data Element Framework: can identify places during a disaster that lack supplies and supply them; convergence of semantic naming and identification technologies; query crew, passenger and cargo list of ship coming in, RFID is about unique id of physical object

SAW: Core Ontology: look like data model but they capture the fact that there are multiple relationships, battlefield resupply scenario: need to know what supplies are where and what is uncertainty of delivering to battlefield:

Semantic Wiki: improves upon in 1. supports operating in Word like environment on the web; better printout and formatting 2. support for ontologies with Visual OWL; Web Ontology Language; looks like Protégé and works on the web and more effectively;

Can work on in three ways: 1. can use better features; 2. go to visual OWL and pick ontologies that you would like to use and drag those out into environment; they are templates for building data; 3. can program and work with the.

Want to see major application built on this platform; is like an operating system on the network; works with semantics rather than code; not sensor network but data being inputted at distributed locations and then correlate.

Net-Ready CBRN Sensors, Joshua Pressnell, JPEO-CBD SSA

What is net-ready to JPEO-CBD? Transformation enabler, empowers users to easily discover, access, integrate, correlate, and fuse data;

Easy to use for Warfighter, using a PDA, watching DATA, doesn't worry about sensors or network; info relevant to their Area of Responsibility; quickly deploy assets with minimal setup; easy access to wireless; PnP; seamlessly disconnect sensors.

Common software services built upon common data model, common schema, and common protocol; need to use modular building blocks; need reuse; component configuration and deployment and dynamic software load provisioning.

Discovers who is online; share info; don't worry about underlying technology; key requirements: need standards to be widely accepted; need groups to mandate standards.

Sensors sense and components deal with network communication, storage, etc.

Scaleable PnP architecture secure over internet

Mounts on vehicles and can dismount while maintaining connectivity to network

Out of the box, should be like turning on any other new item into computer

CBRN sensors will be accessible via W3C open web service standards, need teeth behind mandates, no commercially viable source for standardizing; need to communicate using CBRN XML schema;

JWARN component interface device: brings old sensors into network in common way; tell manufacturers that their devices need to just plug-in

Information Assurance: everyone needs to do it: ability to plug in encryption/decryption on XML

Common Net-Ready RFP and Contracts Language:
A common specification for future JEO-CBD programs; adding networks to traditionally non networked things, make sure that standards are available to these people

Programs need to know how their architecture has to relate to standard/other programs

Security needs to be standardized for all requirements

Hard to get small, diverse sensor companies to develop new standards unless they have funding; if they want to work for DoD then they will comply; they should only need modular component;

Day 2

8:30-9:15: Harmonizing Frameworks for Sensor Networks, Arjun Shankar, ORNL

An architectural framework is…

1. A posited design principle or methodology for constructing and studying architectures
2. Common, pragmatic guidelines for designing architectures to enable comparison and integration
3. A progressive formulation

A framework is not…

A single, monolithic solution
An end state
A tool prescription
A static process

Harmonization: how to work within array of standards

Flow of net ready sensors: edge/sensors then node/gateway then local/regional server; all use http, transport TCP, link/network IP, this raises both infrastructure and data interoperability concerns.

Sensor does work at physical layer of network via sundry mechanism, several hops and reaches first gateway, want intelligence available at gateway, then bring down driver from server to talk with sensor, step of determining intelligence layer of sensor adds layer to stack; in net ready world cross different stack layers as data becomes available, need to be concerned with end to end pipeline of stack

HIS OBSERVATION: unlike in networking pipe, in sensors physical world becomes relevant at different stages of model, intelligence needs to look into data to respond locally or take decisions to other parts of network: this raises the interoperability concerns

Progression of sensor network: Physical interfaces, network, data formats and schemas, services, application interfaces

Need to translate from interfaces to sensors; make sensor data available in web services context using a hardware/software system

SensorNet framework: standards-based, continuing prototyping experiments, many deployments at Port of Charleston and weigh stations

Deployments of Fort Bragg: example of SensorNet framework at Fort Bragg: bringing in commercial vendors who adopt standards according to SensorNet framework: are having success in having commercial vendors buy into wide area sensor framework

WHY is a systematic standards harmonization important? Ebb and flow of subcomponents leads to new device techniques, so need new standards: It is necessary to determine what standards. XML helps standardization but need other answers. Need solution that can change over time.

WIDE AREA INTEROPERABLE SENSOR NETWORK
Need to do fine-grain searches over network, needed more than XML to do XPath searches, had to write new version of XML of sorts

Have to look at different ways of looking at standards: different communities have different missions, need to look at what areas that you need to bring together from each of work areas

WHAT? Delineate functionality: 1. data: unify data models 2. Control: systemize alert levels and semantics or actuation: develop common language for control signals, 3. management: identify similar management information databases 4. Operational Components: software and hardware

WHICH standards to choose? Sensors Meta data uses IEEE 1451 and SensorML; alerting candidates are Sensor Alerting Service and Web Notification Service, as the data leaves the regional system, needs to fit with CAP and EDXL;

WHERE do you locate harmonization?, need smart sensor physical interfaces and edge based local services, and edge to middleware services.

WHEN? at design time: define the standards you will you use that interoperate well, AT IMPLEMENTATION: include translators, develop network centric system

Possible explanation for network centricity's attraction: software interoperability has been software developers problem for a long time, middleware emerged, but under hood interoperability was done by network model under CORBA, need to separate producer-consumer to clean up the interaction, THE network is a clarifier and simplifier.

HOW hardest question: Do thorough background search of available standards; implementation mechanism: define and map vocabulary, syntax protocol: design translators and wrappers; Semantics: mandate ontologies and conceptual schema representation,

Map ANSI concepts 1:1 to GML, that is N42 to GML for SensorNet
DEMONSTRATION:

Example of a net-ready sensor network system: using small form factor cards or boards and connect them to legacy platforms, show proof of concept of self identification: device (laptop) downloads driver to a particular sensor, APD 2000 Chem Sensor handheld, easy to slip in old board and put in tiny sliver of code; uses generic standard using 1451.5 and a wired wireless interface connecting to the Internet: finds and downloads driver: can add single card to sensor and show plug and play

Driver in computer talks to sensor and accesses location automatically.

Fundamental research questions to make this happen: need to find way to find, identify, and name devices: have ways of doing it but don't know how to do it.

SUMMARY: systems development will inevitably involve a wide variety of standards; harmonizing them will be a recurring objective; interoperability is the way to harmonize, Harmonize by: identifying dimensions of interoperation, choosing a network centric model of interaction.

COMMENT FROM PAUL ?: don't know what is plugging in to sensor network unlike plugging into laptop when you know what you plug in, ID is challenge.
Need protection, key management that current protocols can't handle.

REPLY: ID is harder than just giving out passwords and IDs, needs to be addressed.

COMMENT: What are you using in demo? Is it secure?

REPLY: It is ZigBee, web services fit in.

COMMENT FROM ART BOTTERELL: Sensing with whose standards becomes zero sum game: That is not in the best interest of the community.

Run time implementation is key: is bridge between semantic web/ontology layer of interaction and real word action;

SensorNet can function as bridge; must decide which run time standards.

9:15-10:00: SensorML and SWE, Mike Botts, University of Alabama: Huntsville

SensorML is a definition of models and XML schema for describing processes, it models processes for sensors, hardware based measurement and converts them into a digital number.

Vision: ability to discover sensors and processes; also observation lineage, tells whether observation is trustworthy;
On-Demand processing: derivation of higher level information with a priori knowledge of the sensor system;

Supports intelligent sensor networks, is sensor and network friendly and extensible

Designed to manage a wide range of sensors: lots of soft typing, serves as a means for sensor to become known on the web: everything is modeled as a process

Fundamental things about process: input output parameters and taking knowledge out and using it.

Metadata brings about discovery: but it is not for process execution. It includes: ID, classification, description, security constraints, capabilities, contacts, and history.

Want to take processes and put them into chains, then go into an entire system, components and systems make it not process but something physical: aids connectivity and geographic identification

Can be used on left and right side: left side describes how existing data was obtained and makes observations. Right side: what can to do with observation.

In SensorML can package up an algorithm in that can be sent out to define how to do real things: this is where interoperability shows up.

Replacing DIMAP with SensorML, package parameters at image in time, package time instance of a process; and it is a process factory: can plug time values in using SensorML

Left side: weather measurement: then digital numbers (data stream) need right side to use process chain to come up with something useful

Is a soft-typing approach: instead of putting everything as elements; put a qualifier that defines a term in a dictionary, can point to dictionary for long forms of identification

General Detector Model: potentially a very complex process model, all parameters are expressed as curves; efficient way of describing spatial data

On an aircraft: have GPS, altitude sensor, all things all over aircraft need to describe their relationship, SensorML defines process model and tells you latitude longitude and altitude: took raw data from plane's sensor, use SensorML processing to show geolocation and account for pitch and roll; software does not need to know SensorML, it just runs it;

STATUS: approved as of July 24 as V0.0 specification; now has formed revision working group, then after fixing with recommendations will become v1.0.

Plan to have open source process models; want to write white papers to teach how to use;

N42.42 is compatible with SensorML, mapping with 1451 is underway; initially, it seems to be compliable with CBRN data model

Summary: vertical way of dealing with info: readily accesses sensor observations and tasks sensors; could subscribe to alerts when a sensor measures something important.

OGC web services is in test-bed 4.0

Sensor Model Language: not packaging of observation: process of how observation came to be: Observations and Measurements, and Transducer ML

Harmonizations: OASIS Cap being considered as an encoding as portrayal of sensor alert, looking at OASIS EDXL as envelope for alert, looking at IEEE 1451 for PnP

COMMENT FROM RON LAKE: soft typing requires a large registry and assumes that one exists; URNSs are not currently resolvable.

QUESTION: What countries will use it?

REPLY: NASA and MGA have used and several government contractors are involved at bringing it into DoD and some foreign militaries have agreed to use, Homeland security not fully engaged.

10:15-11:00 PnP-X and WS-Discovery, Jack Timmons and Dave Roth, Microsoft

Goals:
1. Effortless: network connected as easy as USB; lower cost to develop and support
2. Secure: Enable secure transfer of information
3. Rich experiences: platform for the next wave of innovation

Solution: web services on Devices: DPWS device profile for web services, cross internet connectivity for devices

Lightweight version of enterprise (100k)
Security: SSL/TLS and WS-Security

Windows Rally: services on PC that help with web services on devices: windows connect network: easy home network setup; Windows Plug n Play (PnP-X); Development tools (WSDAPI); diagnostic tools (Link layer topology discovery LLTD-Map); quality of service (LLTD-QoS)

Web services on devices: Discovery: problem everyone has for devices if they want PnP; want to detect small devices (sensors, printers, scanners) Indigo: communicate with large services; small devices don't have memory to manage; devices profile for web services: cut out pieces not needed to make small devices work;

Spec is WS-Discovery for small devices: small devices announces self using WS-Discovery protocol when it decides to leave it announces that it is leaving; more active discovery that machine can go out and find all of the sensors or printers on a network: sends out probe for all printers: all of them respond: machine would resolve address of printer: machine connects to device to get metadata: Client machine has enough info to control through standard web services.

Client can subscribe to events, if certain event happens, client is notified for events of interest

Control and eventing: contract defined by WSDL and XML schema; ensure common baseline for interoperability; uses standard WSDL/1.1

Presents rich eventing model, allows for detailed events, client subscribes; host can stop them from subscribing to events: both are securable: uses HTTPS; standard certificate exchange sends out to both sides; access control based on certificates

WS-Security: compact signature; secure channel based on TLS provides encryption; does not support WS-Discovery, instead uses HTTPS URN

Deliverables: WSDAPI shipping in Vista, beta available now: beta toolkit available Fall 2006: planning for XP, Windows Server next year

WSDAPI shipping in WinCE: projector support shipping September 2006; general support in December 2006

WS stack on .NET Micro Framework: shipping in Dec 2006

Linux stack currently available from various partners

Product pipeline: Vista PCs no longer use net BIOS; now use WS-Discovery; working with printers and scanner companies to use networking;

RFID readers will get Discovery

Standards: will be RAND-Z, evaluating internet standards organizations: OASIS or W3C or ECMA; work with partners to determine best standards organization per device class; Process: create with SDLs in industry with leading partners, drive products to market, then check it into standards organization: fast track process

COMMENT FROMRICK MCMULLEN: IP4 multicast, not very reliable outside of a room, is that a design problem, that why do you have proxies, Why use it to begin with?

REPLY: Restricted to a single subnet, necessary for consumer, don't want ambient traffic noise; proxy has a footprint in every subnet, tells proxy not to multicast, proxy can cache responses or re-query each thing, Proxy is a good thing for network traffic issues.

COMMENT FROM BRAND NIEMANN: IPP6 address needed for government

REPLY: Windows Vista will work in everything with IPP6; Discovery works with it; WSD on Vista will totally support it

COMMENT FROM BRAND NIEMANN: Will it use an ontology to find it? First come first serve is not as organizable; need an ontology to handle routing of telephone calls, need to allocate according to hierarchy or ontology.

REPLY: WS-Discovery: flat system: everyone announces and makes noise: if proxy based could use this type of hierarchal system; Discovery could use logic. Even if not proxy, metadata within each probe request could define what type.

QUESTION: What is required at device level to support this stack?

REPLY: Technical requirements are stack dependent; 200-300k range some say 100k, some 60k, XML parser, sub parser, HTTP.

COMMENT FROM ART BOTTERELL: Thanks Microsoft for using CAP, says Microsoft has a new level of sensitivity to standards issues.

11:00-11:45: Sun SPOT, David Simmons, SUN

A sensor with a powerful processor and 802.15.4 radio with antenna; it is the IEEE standard instead of ZigBee

Sensor board: 3 axis accelerometer; light sensor; temperature sensor; 8 tri color LEDs for display; 5 GPIO pins for external I/O control; 2 switches, and USB

Provides the ease of JAVA for development deployment and debugging, all programmed in JAVA, stable, robust and widely-accepted language and tools, can develop applications right away;

Prototypes are usable today: wireless networking, robotics, industry, monitoring, military and security applications

Any type of sensor can be put on it; Gore makes penetration detection fabric; using accelerometer to detect movement

Wants to make it a software problem; can solve hardware problems using software; non EE students can build operation devices; quickly implement a prototype; focus on solution not process of what you need to build to get there.

Runs on Squawk JAVA OS; floating point; executes directly out of onboard flash;

SPI interface can build own sensor board; standard connector; can talk to it through SPI, to abstract through JAVA OS, tell it to get SPI driver; or use a microcontroller code that you write and java can program it within JAVA

QUESTION: How much current from battery?

REPLY: 720 millivolt battery; has snooze mode; deep sleep: only thing running is timer; would last about 13 months if wake up about once a week; don't have to shut it off yourself; JAVA OS will shut stuff down by itself; don't do power management yourself

QUESTION: What would a quantity of 1000 cost?

REPLY: In two weeks will be selling development kits of two Sun SPOTS and PC hookup for $500.

Ways to sign JAVA loader and authenticate before you load: had to do it before they could use JAVA, must be secure code deployment; range is around 100 meters

Try to use standards and standards based protocols; ships with Netbeans and other demos;

What distinguishes this device: size, computing power and JAVA; have run a web browser and an RSS feed

1:00-1:45: IEEE 1451.0/5, Kang Lee, NIST

Smart sensor interface standards; 1451.0 is of more interest for sensors, 1451.5 is wireless

Why sensor standards? He worked as sensor engineer; hard to connect. Wanted to make sensors easier to use. Eventually could be many sensors, even if cheap must achieve connectivity and share information. Need good information exchange or will waste time converting signals. Open standard interface and data formats are keys for Homeland Security applications.

Customers want open standards; if they require it company will want it. As a user you want to pick up a sensor, easily plug it in, and self identify to network: that is why they wrote 1451: interoperability.

Goal made in 2004 at SensorGov Conference to eliminate non-integrated sensors by FY08 and use commercial standards instead of military standards; but Military can help to drive

Integrated network sensors: low cost yet PnP; sensor manufacturers are not network experts, they just want to work on sensors so they devise it into two: Transducer Interface Module (TIM) which does signal conversion has a digital interface with NCAP which processes data. Network capable Application Processor, which tasks to any network.

Transducer interface is wired or wireless and standardized, as is data format and common commands: do not want to standardize actual sensing technologies and codes and processors, Transducer Electronic Data Sheet TEDS, it can identify itself even if it is an old sensor that doesn't work

1451.0 are common command sets either wired or wireless, 1451.1 Smart Transducer Neutral Model, can talk to sensor and network

IEEE 1451, a suite of Smart Transducer Interface Standards, a set of open, network independent communication interfaces for connecting transducers to microprocessors, instrumentation systems, and networks. TED is quite large but it is scalable, only 4 mandatory things: basic manufacturing information, transducer channel TEDS, User's transducer name TEDS, and PHY TEDS, which is very few bytes ~100 or ~200, can have much more information, for things like Geographic location; network neutral and vendor neutral.

Most of them have been published, 1451.5 is in balloting. 1451.1 will be revised;

1451.0: common interface for talking to physical layer of sensor , does discovery and writes and reads the TED, can also do TIM discovery;

managing TED: If user changes characteristics of TED then the changes are written onto it.

Sensor web services based on 1451: TIM Discovery Services; Sensor Observation Services; Sensor TEDS services

Provides Common functions: Hot swap capability; status reporting; self-test capability service request messaging, synchronous data acquisition; stack chart: three paths to the internet: sensor web services, 1451.1, or HTTP 1451 web applications

IF you do HTTP protocol then you get HTTP request then response depending on what you are requesting; response could be in XML ASCII text or binary;

Will include multiple PHY and MAC standard wireless protocols in the proposed standard, will adopt Wi-FI, Bluetooth, ZigBee and IPv6

Each PHY/MAC combination provides a higher layer API interface for seamless interoperability with IEE 1451.

WIFI, ZigBee, and Bluetooth have their own native ways of handling security and key exchange.

Working with Sun to work into Sun SPOT platform

Benefits to using IEEE 1451:
Standard interface for manufacturers
Multiple products may be developed just by changing the TEDS.
Standard calibration specification

System integrators:
Self documenting hardware and software
Systems that are easier to maintain
Rapid transducer, easier to put things together

Easier for users to use

Sensor Standards Harmonization SSH Working Group: a forum for industry, academia and government to exchange information about the various sensor related standards being developed.

Identify opportunities to frame the harmonization of sensor-related standards to meet the need of the community.

NIST agreed to lead the effort and organize quarterly working group meeting at NIST on the third Tuesday of the month staring December 2005; next meeting is September 12, 2006.

Joint Test-beds: like IEEE 1451 OASIS and OGC; need to be developed and implemented to accelerate standards development and ID gaps. Funding should be identified to leverage near term test-bed activities.

Government should specify relevant sensor standards in procurements. This will accelerate market provision of PnP systems which will cover costs and allow for easier upgrades than proprietary systems.

Government should encourage standards organizations to collaborate.

The group will do gap analysis: consistent accurate methodology for defining location in content objects of EDXL payload (OGC standards may offer a solution), and will affirm standards capability and identify gaps for further work

QUESTION FROM JACK TIMMONS: Does it have IPv6 stack?

REPLY: It is proposed but is not accepted yet.

1:45-2:30: CIMA, Rick McMullen, Indiana University

Common Instrument Middleware Architecture (CIMA)

CIMA project goals: supported by the NSF middleware initiative;
Wants to institute instruments and sensors as real-time data sources into grid computing environments through a service oriented architecture: also improve accessibility; promote sharing in hardware facilities

Develop a methodology for describing instrument capabilities and functions and embedding these in the hardware to improve flexibility and lifetime of data acquisition and analysis applications

Move production of metadata as close to instruments as possible and facilitate the automatic production of metadata and improve data management and reuse

Components: service architecture: IR code which is device independent; plug ins and drivers that are device independent; service life cycle high level protocol, communications self description, discovery and security, proxy service and embeddable code and client coding practices

Communications protocol: transport-neutral, standards-based

Instrument and sensor description: ontology-based but capable of updating the information instrument that the hardware already has; should be able to build functional model from description; description instance development parallels plug-in development Ontology should be extensible as a community effort.

Web services interfaces out in the field register with a registry service; data acquisition code can locate and notify with registry; helps create easily extensible networks; DAC can then query hardware for instrument description and they can have a request/response interaction. Can do events and streaming data if it wants.

Design Considerations:
Prefer IP accessible devices IPv4 or IPv6 but support bridging to other buses like ZigBee, Motes RF protocol, RF modems, CANBus,
Uses well know transport protocols like SOAP over HTTP/S
But support alternatives like WS-X, Jabber, Antelope; supports unreliable or intermittent connectivity: gives message persistence to messaging services

Prefer “proxy” approach for CIMA service implementation for richer capabilities set and less impact on existing instruments but support embedded systems though C++ and cooperative use of instruments at the semantic level

Want integration with emerging Grid Computing standards for SOA

Sensor networks example: ecological observations like on lake buoys by Long Term Ecological Research group and with MOTE sensor package; these use CIMA

CIMA service has a TCP network at bottom with channel (WS plus parcel protocol) and connects with Plug in who connects with sensor and commands are sent to the sensors/actuators.

Instrument metadata describes hardware and map ins between plug ins and provides hooks for real-time annotation of data

Maps, sensors, and actuators are defined in plug ins

Applications can query the instrument description to build an operation model of the instrument on the fly

Description instance based-on ontology, which can be put into XML

Ontology in OWL-DL: good for machine reasoning; allows for consistency checking at semantic level, future application in machine reasoning

Provides classes and properties for identifying the instrument or sensor’s physical location; service location in communications space and pragmatic info about how to acquire the data

CIMA Channel Protocol: simple web services interface: one endpoint at instrument or one at client both are string type

SOAP payload is a Parcel XML document or fragment; REST-like protocol using document oriented SOAP messages (parcels): like describe, register, get, and set

Additional layered specifications can be added as needed like WS-security and WS-Addressing

Protocol can be extended by versioning the parcel schema without modification to older clients or instrument services;

Clients can request data on multiples steams at different rates: one instrument service supports multiple clients

Binary XML or gzip compression can augment SOAP

PARCEL data structure: receives and sends Parcel XML documents: content has header info including body containing request parameters

High level use case: producer then intermediary then consumer model, needs routable structures that intermediaries can forward without completely parsing

Suitable for resource constrained wireless sensor networks and source routing protocols

Security (SOAP/HTTP): SSL, WS-Security or other SOAP message encryption schemes; Firewalls that allow HTTP or HTTPS

Access control: output filtering by IP address ; can cut people out by forbidding them to access data.

Looking at external role authorization using SAML and Shibboleth or PERMIS

Transport: WSDL defines a transport binding per port

Intermediaries can be used like RSS or CAP; can be transport converters from http to a publish/subscribe system

CIMA in processing pipelines: scenario where sensors a and b combine instruments to get an augmented set of capabilities that provides consumer with an alternate view of the hardware; data flow and service orchestration: CIMI requires manually implemented data flows

CIMA can extend in-house capabilities: can use underlying EPICS control as backend for a CIMA device that will extend data to clients

Implementation issues: Location issues: WFS is interesting, Security: at each node and at transport level; Authentication

Aggregation and transformation of real-time data streams: want to look at composite instruments with domain specific interfaces

Integrated with SensorNET at ORNL

COMMENT FROM RON LAKE: WSDL cannot see what it is other than shipping parcels around.

REPLY: You have little insight into what they do unless you look into them yourself. Can be seen as a positive.

QUESTION FROM RON LAKE: CIMA has “ontology-light” with WFS, but have you looked at proxying out from low bandwidth sites and only using higher bandwidth to do additional services.
REPLY: decided to specify DTN2; entirely possible but have not found right application

COMMENT FROM MIKE BOTTS: recommended SensorML: thought indirect typing might be good;

Net-ready Sensors Workshop notes – Hixson/NG9-1-1 edited

2:30-3:15: Next Generation 9-1-1, Roger Hixson, NENA

The current 9-1-1 system is possible because of standards that were brought together to make it ubiquitous. 9-1-1 centers are Public Safety Answering Points (PSAPs); 5,700 primary PSAPs in about 3200 Counties.

Sensor data usable for 9-1-1 centers must be:
Discoverable when needed
Automatically routable or accessible based on location
IP compatible
XML based
Interpretable quickly

Questions about what system should be: Secure vs. public: subscription, activation, etc.

It is location based so you must route to right place.

Today's E9-1-1:
Designed in mid 70s, it is analog and uses switches
It was designed for land lines and for low cost; off the shelf components;
ILECS (Incumbent Local Exchange Carriers)
CLECS (Competitive Local Exchange Carriers)
Private switches via both ILECS and CLECS
Cellular wireless carriers
VOIP came around, too
Cable tv calling systems: use private systems, not internet for 9-1-1

Components: originating calls, switching centers, routers, primary PSAPS and secondary PSAPS: About 300 of these networks around the country (routing centers to PSAPS)

Router looks at location related database to determine who it needs to send call to. Most of the databases are unique to this process

It is difficult and costly to integrate new call or messaging sources and the corresponding data needs with the current design of the E9-1-1 system.

Routing process is fundamental; adaptations of the current E9-1-1 cannot effectively support 9-1-1 needs, so need to change system

Upcoming and unknown devices with IP interfaces; what should the target for the future be? End to end IP based E9-1-1; critical to verify assumptions against E9-1-1 functionality: cannot drop back from old live system; so hampers testing of a new system

Needs to be verified and tested exhaustively before it is put in place; must be seamlessly linked with other evolving emergency systems

IP based E9-1-1 (NG9-1-1) must support all technologies like VoI, general VoIP, WiFi, WiMax, ILEC and CLEC, cellular MSCs, satellite systems, text messaging, emergency data

Principles of design: support dynamic, flexible, Open architecture System design process for 9-1-1; Compatible with the commercial environment for IP Communications; Must promote a fully funded 9-1-1 system; Need to simplify architecture compared to today's system

Structure for NG 9-1-1: a really secure firewall between general Internet and 9-1-1 IP Net. ILECS, CLECS, MSCs, other emergency services providers, CAD mapping and radio plug into E9-1-1 IP NET directly; VoI goes through high security firewall

I3 Proposal: PSAPs will be on a private IP network

Fixed, nomadic and true mobile clients are supported

Multiply media types like voice, text, indicator data, and video

International operation supported

No assumption of e.164 telephone number addressing; No specific carriers presumed

280+ requirements have mostly been completed; a few tweaks but nothing major; formal review is about to start; being utilized in Texas A&M trial

Want to implement by 2009, but funding is a major problem.

COMMENT FROM ART BOTTERELL: central database goes away; reverse 9-1-1 services have an issue; are emergency notifications negatively affected? Who will handle selective routing function?

REPLY: There will be within the network a way to validate locations, but it is an open question. Emergency notification will actually be eased due to new capabilities in NG9-1-1. Selective Routing function becomes a software technique. Does not think standard telephone companies will do it.

COMMENT FROM RICK MCMULLEN: Who will do network engineering?

REPLY: Whoever manages the Emergency Communication IP network for a given geographic area

QUESTION: What government agency is the effort a part of?

REPLY: Federal ICO: Established in 2004 as joint office of the Department of Transportation and the National Highway Safety Administration. But other agencies have roles, such as DHS, DoJ.

3:30-4:00: Workshop Wrap-up: Bryan Gorman, ORNL

Commoditizing the infrastructure between the sensor and the applications to make the connections as seamless and as inexpensive as possible is a goal

User community has an appetite for sensors and a requirement for standard.

Issues: Navigating the Standards maze, many standards related orgs
Everyone feels like they have a solution; need for harmonization.

Need to start with simple foundation and principle.

Hard to predict which standards will be accepted; coming together and talking helps; not doing work in isolation; transparent and open platform makes it easier to know what will happen. Harmonization meetings will also make it better. Need to reach across to colleagues. Need to bring together energies toward a common goal.

Need to be able to absorb new technologies. Must understand it and express it in technical terms.

Avoid proprietary interfaces. Be open and interoperable.

Work towards long term global solutions, but build in very small increments. Maintain optimism.